REMARKS

This amendment is responsive to the above identified non-final Office Action. Claims 14 - 92 are now pending. Claims 14 -17, 22, 27, 32, 37, 42, 47, 52, 57, and 62 have been amended to more particularly point out subject matter which the Applicants regard as their invention. No new subject matter has been added.

I. Rejections Under 35 U.S.C. § 112

Each of the independent claims 14-46 have been rejected under 35 U.S.C. § 112, first paragraph. Claims 14 and 15 have been rejected under 35 U.S.C. § 112, second paragraph, as failing to point out and distinctly claim the subject matter which applicants regard as their invention.

Claims14-16, 22, 27, 32, 37, and 42 previously recited the provision of being "backwards compatible with preexisting public key infrastructure ...." Applicants have amended each of these claims to recite the provision of being "... backwards compatible with preexisting public key *transformation schemes* ..." in order to make it more clear that this subject matter is supported by the description on page 7, lines 12-16 of the original application which recites that "[o]ther advantages of the invention include its employment for decryption without the need to revise the RSA public encryption transformation scheme currently in use on thousands of large and small computers." Each of the independent claims 47, 52, 57, and 62 has also been amended to include the provision of being "backwards compatible with preexisting public key infrastructure ...." Applicants submit that the original specification provides adequate support for the amendments to each of the claims 14-16, 22, 27, 32, 37, 42, 47, 52, 57, and 62.

Claims 14 and 15 have been rejected under 35 U.S.C. § 112, second paragraph, as failing to point out and distinctly claim the subject matter which applicants regard as their invention. Each of these claims previously recited a "minimal amount of computer instructions." Claims 14 and 15 have both been amended to recite "... whereby said step of decoding <u>is accelerated</u> ..." in place of "... whereby processing of a minimal amount of computer instructions is required for said step of decoding ...." Applicants submit that the amendment now clearly points out that the step of decoding is fast and efficient as the Examiner correctly assumed for purposes of the present Office Action (see Examiner's comment on page 4, lines 4 and 5).

In light of the above described amendments and remarks, Applicants submit that all of the claims 14 through 46 now satisfy the requirements of the first and second paragraphs of 35 U.S.C. § 112. Applicants thank the Examiner for careful review of the claims.

II. Rejections Under 35 U.S.C. § 102

Claims 14-66 have been rejected under 35 U.S.C. § 102(b) as being anticipated by Rivest et al. (US Patent No. 4,405,829). The Office Action states that "... the applicant's invention is particularly directed to ..." (1) using more than two primes in the modulus, and (2) using the Chinese Remainder Theorem to speed up decryption. The Office Action points specifically to column 13, lines 29-34 of Rivest et al. which states that,

> "In alternative embodiments, the present invention may use a modulus n which is a product of three or more primes (not necessarily distinct). Decoding may be performed modulo each of the prime factors of n and the results combined using "Chinese remaindering" or any equivalent method to obtain the result modulo n...."

The Office Action further states on page 4, last paragraph, that "... the particular equations specified in claim 14, lines 11-24 and 30-32, and in the corresponding parts of other claims, are inherent in using the Chinese Remainder Theorem for decoding ...."

Claim 14 specifically recites the step of,

> "... combining said results of said subtasks in accordance with a fast recursive combining process to produce said ciphertext word signal C whereby,
>
> $Y_i \equiv Y_{i-1} + [(C_i - Y_{i-1})\ (w_i^{-1} \bmod p_i) \bmod p_i] \cdot w_i \bmod n$
>
> $2 \leq i \leq k$, and
>
> $C = Y_k,\ Y_1 = C_1,$ and $w_i = \prod_{j<i} p_j$ ...."

The Office Action states that these particular relationships are inherent in using the Chinese Remainder Theorem as taught by Rivest et al. However, the Office Actions provides no explanation or support for this position. Applicants respectfully submit that the above cited relationships are not "... inherent in using the Chinese Remainder Theorem ...." The Chinese Remainder Theorem itself does not provide any actual solutions for solving a system of multiple linear congruencies. It merely states that a solution must exist for solving a system of multiple

linear congruencies under certain conditions. Applicants acknowledge that various types of recursive and Gaussian solutions (Chinese Remainder Algorithms) have been applied to two prime RSA encryption schemes. However, Applicants point out that none of the cited references teach an application of any Chinese Remainder Algorithm for practicing a multi-prime cryptographic scheme using a modulus n having more than two primes as recited in each of the independent claims of the present invention.

Rivest et al. merely suggests a desire to use a modulus n which is a product of three or more primes, and perform decoding using "Chinese remaindering". However, as noted in the Office Action, Rivest et al. provides no actual solution, that is no effective Chinese Remainder *Algorithm*, for actually practicing a multi-prime cryptographic scheme using a modulus n having more than two primes as recited in each of the independent claims of the present invention. While Rivest et al. may be interpreted as generally suggesting the desirability or possibility of implementing a multi-prime cryptographic scheme, it provides no actual teaching of how to implement such a scheme. Therefore, Applicants assert that claims 14-66 are patentable under 35 U.S.C. § 102(b) over Rivest et al..

III. Rejections Under 35 U.S.C. § 103(a):

A. Claims 67-92 are patentable under 35 U.S.C. § 103(a) over Rivest et al. in view of Menezes et al.

Claims 67-92 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Rivest et al. in view of Menezes et al. (note 14.87 (iii) on page 617 of the Handbook of Applied Cryptography). Each of claims 67, 69, 71, 73, 75, 77, 79, 81, 83, 85, 87, 89, and 91 recites "...wherein said step of solving said sub-tasks includes processing each of said sub-tasks by an associated one of a plurality of exponentiator units operating substantially simultaneously...." The Office Action states on page 7 that "... Menezes et al. discloses simultaneous multiple exponentiation."

Applicants respectfully point out that Menezes et al. teaches an algorithm (see algorithm 14.88 on page 618 of Menezes et al.) for simultaneous multiple exponentiation whereas each of the claims 67, 69, 71, 73, 75, 77, 79, 81, 83, 85, 87, 89, and 91 recites a structural hardware limitation defined by "...a plurality of exponentiator units operating substantially simultaneously...." The teaching of Algorithm 14.88 on pages 617-618 of Menezes et al. does

not mention "... a plurality of exponentiator units operating substantially simultaneously ...." The algorithm in Menezes et al. includes a step of precomputing (see "step 1. Precomputation ...") and computer program loops (see "step 3 For i from 1 to t do the following ...."), all of which suggests that Algorithm 14.88 is intended to be implemented as computer readable instructions executed over a single processor for the purpose of achieving simultaneous multiple exponentiation. It is clear however, that Menezes et al. does not teach the structural limitations inherent in the language "... a plurality of exponentiator units operating substantially simultaneously ...." The specification of the present application provides support for the exponentiator units on page 13, lines 10-20.

Applicants assert that none of the cited references teaches "... a plurality of exponentiator units operating substantially simultaneously ...." Therefore, applicants assert that claims 67, 69, 71, 73, 75, 77, 79, 81, 83, 85, 87, 89, and 91 are patentable under 35 U.S.C. § 103(a) over Rivest et al. in view of Menezes et al.

B. Claims 14-92 are patentable under 35 U.S.C. § 103(a) over Menezes et al. in view of Quisquater et al.

1. Neither Menezes et al. nor Quisquater et al., taken either individually or collectively, teaches, hints, or suggests a cryptographic scheme using a composite number having more than two primes.

Claims 14-92 have been rejected under 35 U.S.C. § 103(a) over Menezes et al. in view of Quisquater et al. The rejections of claims 14-92 under 35 U.S.C. § 103(a) rely on an assumption that Menezes et al. teaches a cryptographic scheme using a composite number having more than two primes. As explained in response to previous office actions, Menezes et al. is a well known textbook that describes conventional cryptography techniques and elementary number theory. The expression in Menezes et al. of the integer factorization problem (definition 3.3 recited on Page 89 of Menezes et al.) merely recites a fundamental theorem of arithmetic which states that: "$n = p_1^{e1}p_2^{e2}...p_1^{ek}$ where the p_i are pairwise distinct primes and each $e_i > 1$".

This fundamental theorem of arithmetic, which has been known for centuries, appears in every text book that addresses number theory. This theorem merely states that all numbers are either prime or composite, and that all composite numbers have a unique factorization as a product of powers of prime numbers meaning that a particular composite number cannot be

formed as a product of a different set of primes. For the above explained reasons, Applicants assert that the expression "$n = p_1^{e1}p_2^{e2}...p_1^{ek}$" does not even remotely suggest a solution to the problems associated with actually implementing a "multi-prime" cryptographic scheme using a composite number having more than two primes. For the reasons stated above, Applicants assert that Menezes et al. does not teach the possibility of a multi-prime cryptographic scheme using a composite number having more than two primes.

2. Neither Menezes et al. nor Quisquater et al., taken either individually or collectively, teaches, hints, or suggests use of a Chinese Remainder Algorithm for solving subtasks in a cryptographic scheme using a composite number having more than two primes.

Although Menezes et al. provides general teachings of Gauss's algorithm and Garner's algorithm for solving simultaneous congruences, Menezes et al. does not teach any specific application of these algorithms for solving subtasks in a cryptographic scheme using a composite number having more than two primes. Applicants further assert that neither Menezes et al. nor Quisquater et al. provides any motivation to solve subtasks in a cryptographic scheme using a composite number having more than two primes

3. Neither Menezes et al. nor Quisquater et al., taken either individually or collectively, teaches, hints, or suggests use a cryptographic scheme using a composite number having more than two primes *wherein the scheme is backwards compatible with preexisting public key transformation schemes.*

Applicants do not understand the statement on page 11 of the Office Action which recites "[t]hat the well-known RSA cryptosystem is a special case of the above combination indicates that it is backwards compatible with RSA." Applicants assert that this statement is not supported by any fact.

Page 7, lines 12-16, of the present application states that "[o]ther advantages of the invention include its employment for decryption without the need to revise the RSA public encryption transformation scheme currently in use on thousands of large and small computers." Applicants assert that neither Menezes et al. nor Quisquater et al., taken either individually or collectively, teaches, hints, or suggests a cryptographic scheme using a composite number

having more than two primes wherein the scheme is backwards compatible with preexisting public key transformation schemes.

Each of the independent claims 42, 47, 52, 57, and 62 has been amended to recite the provision of being "backwards compatible with preexisting public key transformation schemes ...." Therefore, all of the independent claims 14-16, 22, 27, 32, 37, 42, 47, 52, 57, and 62 recite the provision of being "backwards compatible with preexisting public key transformation schemes ...", and as such are patentable under 35 U.S.C. § 103(a) over Menezes et al. in view of Quisquater et al.

Attached hereto is a marked-up version of the changes made to the claims by the current amendment. The attached pages are captioned "**VERSION WITH MARKINGS TO SHOW CHANGES MADE**."

In view of the foregoing amendments and remarks, it is submitted that the application is now in condition for allowance and a notice of allowance of the pending claims 14 through 92 is respectfully requested. In the event that a telephone conference would expedite prosecution of the application, the Examiner is respectfully invited to contact the undersigned by telephone at the number set out below.

Respectfully submitted,

Dated: June 13, 2001
OPPENHEIMER WOLFF & DONNELLY LLP
Customer No. 25696

Justin Boyce
Reg. No. 40,920

CERTIFICATE OF MAILING (37 CFR 1.8(a))

I hereby certify that this paper (along with any referred to as being attached or enclosed) is being deposited on June 13, 2001, with the U.S. Postal Service as First class mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C., 20231.

Date: June 13, 2001

Yolette Yturralde-Owen

VERSION WITH MARKINGS TO SHOW CHANGES MADE

In The Claims:

14. (Three Times Amended) A method for establishing cryptographic communications that are backwards compatible with preexisting public key [infrastructures] transformation schemes, comprising the step of:

encoding a plaintext message word M to a ciphertext word C, where M corresponds to a number representative of a message and

$0 \leq M \leq n-1$

n being a composite number formed from the product of $p_1 \cdot p_2 \cdot \ldots \cdot p_k$ where k is an integer greater than 2, and $p_1, p_2, \ldots, p_k$ are distinct random prime numbers, and where the ciphertext word C is a number representative of an encoded form of message word M, said encoding step including the steps of,

defining a plurality of k sub-tasks in accordance with,

$$C_1 \equiv M_1^{e_1} \pmod{p_1},$$

$$C_2 \equiv M_2^{e_2} \pmod{p_2},$$

$$\vdots$$

$$C_k \equiv M_k^{e_k} \pmod{p_k},$$

where

$$M_1 \equiv M \pmod{p_1},$$

$$M_2 \equiv M \pmod{p_2},$$

$$\vdots$$

$$M_k \equiv M \pmod{p_k},$$

$$e_1 \equiv e \pmod{(p_1 - 1)},$$

$$e_2 \equiv e \pmod{(p_2 - 1)}, \text{ and}$$

$$\vdots$$

$$e_k \equiv e \pmod{(p_k - 1)},$$

where e is a number relatively prime to (p_1-1), (p_2-1), ..., and (p_k-1),

solving said subtasks to determine results C_1, C_2 ... C_k,

combining said results of said subtasks in accordance with a fast recursive combining process to produce said ciphertext word signal C whereby,

$$Y_i \equiv Y_{i-1} + [(C_i - Y_{i-1})\ (w_i^{-1} \bmod p_i) \bmod p_i] \bullet w_i \bmod n$$

$$2 \leq i \leq k, \text{ and}$$

$$C = Y_k,\ Y_1 = C_1, \text{ and } w_i = \prod_{j<i} p_j$$

whereby [processing of a minimal amount of computer instructions is required for] said step of encoding is accelerated.

15. (Three Times Amended) A method for establishing cryptographic communications that are backwards compatible with preexisting public key [infrastructures] transformation schemes, comprising the steps of:

decoding a ciphertext word C to a message word M, wherein M corresponds to a number representative of a message and wherein,

$$0 \leq M \leq n-1$$

wherein n is a composite number formed by the product of $p_1 \bullet p_2 \bullet \ldots \bullet p_k$, k is an integer greater than 2, and p_1, p_2, ..., p_k are distinct random prime numbers, C is a number representative of an encoded form of message word M that is encoded by transforming said message word M to said ciphertext word C whereby,

$$C \equiv M^e \pmod n,$$

and wherein e is a number relatively prime to (p_1-1), (p_2-1), ..., and (p_k-1),

said decoding step being performed using a decryption exponent d that is defined by

$$d \equiv e^{-1} \bmod ((p_1-1)\ (p_2-1) \ldots (p_k-1)),$$

said decoding step including the steps of,

(i) defining a plurality of k sub-tasks in accordance with

$$M_1 \equiv C_1^{d_1} \pmod{p_1},$$

$$M_2 \equiv C_2^{d_2} \pmod{p_2},$$

$$M_k \equiv C_k^{d_k} \pmod{p_k},$$

where

$$C_1 \equiv C \pmod{p_1},$$

$$C_2 \equiv C \pmod{p_2},$$

$$\vdots$$

$$C_k \equiv C \pmod{p_k},$$

$$d_1 \equiv d \pmod{(p_1 - 1)},$$

$$d_2 \equiv d \pmod{(p_2 - 1)}, \text{ and}$$

$$\vdots$$

$$d_k \equiv d \pmod{(p_k - 1)},$$

(ii) solving said sub-tasks to determine results $M_1, M_2, \ldots M_k$, and

(iii) combining said results of said subtasks in accordance with a fast recursive combining process to produce said message word M in accordance with,

$$Y_i \equiv Y_{i-1} + [(M_i - Y_{i-1})\ (w_i^{-1} \bmod p_i) \bmod p_i] \bullet w_i \bmod n$$

where $2 \leq i \leq k$, and

$$M = Y_k,\ Y_1 = M_1, \text{ and } w_i = \prod_{j<i} p_j$$

whereby [processing of a minimal amount of computer instructions is required for] said step of decoding <u>is accelerated</u>.

16. (Three Times Amended) A cyptographic communications system for establishing communications that are backwards compatible with preexisting public key <u>transformation schemes</u> [infrastructures], comprising:

a communication medium;

encoding means coupled to said communication medium and adapted for transforming a transmit message word M to a ciphertext word C and for transmitting said ciphertext word C on said medium, where M corresponds to a number representative of a message, and

$0 \leq M \leq n-1$ where n is a composite number of the form

$n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$,

where k is an integer greater than 2 and $p_1, p_2, \ldots, p_k$ are distinct random prime numbers, and where C corresponds to a number representative of an enciphered form of said message, and corresponds to

$C \equiv M^e \pmod{n}$,

where e is a number relatively prime to (p_1-1), (p_2-1), ..., and (p_k-1); and

decoding means coupled to said communication medium and adapted for receiving C via said medium and for transforming C to a receive message word M' where M' corresponds to a number representative of a deciphered form of C, said decoding means being operative to perform a decryption process using a decryption exponent d that is defined by

$$d \equiv e^{-1} \bmod ((p_1-1)(p_2-1)\ldots(p_k-1)),$$

said decryption process including the steps of

(i) defining a plurality of k sub-tasks in accordance with,

$$C_1 \equiv C \pmod{p_1},$$

$$C_2 \equiv C \pmod{p_2},$$

$$\vdots$$

$$C_k \equiv C \pmod{p_k},$$

where,

$$d_1 \equiv d \pmod{(p_1 - 1)},$$

$$d_2 \equiv d \pmod{(p_2 - 1)},$$

$$\vdots$$

$$d_k \equiv d \pmod{(p_k - 1)},$$

$$M_1' \equiv C_1^{d_1} \pmod{p_1},$$

$$M_2' \equiv C_2^{d_2} \pmod{p_2}, \text{ and}$$

$$\vdots$$

$$M_k' \equiv C_k^{d_k} \pmod{p_k},$$

(ii) solving said sub-tasks to determine results M_1', M_2', ... M_k', and

(iii) combining said results of said subtasks by a fast recursive combining process to produce said receive message word M' in accordance with

$$Y_i \equiv Y_{i-1} + [(M_i' - Y_{i-1}) (w_i^{-1} \bmod p_i) \bmod p_i] \bullet w_i \bmod n$$

where $2 \leq i \leq k$ and

$$M' = Y_k,\ Y_1 = M_1, \text{ and } w_i = \prod_{j<i} p_j,$$

wherein M'=M.

17. (Twice Amended) A method for establishing cryptographic communications that are backwards compatible with preexisting public key [infrastructures] transformation schemes, comprising the steps of:

encoding a plaintext message word M to a ciphertext word C, wherein M corresponds to a number representative of a message and wherein

$$0 \leq M \leq n-1,$$

wherein n is a composite number formed by the product of $p_1 \bullet p_2 \bullet \ldots \bullet p_k$, k is an integer greater than 2 and $p_1, p_2, \ldots, p_k$ are distinct random prime numbers, C is a number representative of an encoded form of message word M, and wherein said encoding step comprises transforming said message word M to said ciphertext word C, whereby

$$C \equiv M^e \pmod n,$$

and wherein e is a number relatively prime to (p_1-1), (p_2-1), ..., and (p_k-1); and

decoding said ciphertext word C to a receive message word M', said decoding step being performed using a decryption exponent d that is defined by

$$d \equiv e^{-1} \bmod ((p_1-1)(p_2-1) \ldots (p_k-1)),$$

said decoding step including the further steps of,

defining a plurality of k sub-tasks in accordance with

$$M_1' \equiv C_1^{d_1} \pmod{p_1},$$

$$M_2' \equiv C_2^{d_2} \pmod{p_2},$$

$$\vdots$$

$$M_k' \equiv C_k^{d_k} \pmod{p_k},$$

wherein

$C_1 \equiv C \pmod{p_1}$,

$C_2 \equiv C \pmod{p_2}$,

⋮

$C_k \equiv C \pmod{p_k}$,

$d_1 \equiv d \pmod{(p_1 - 1)}$,

$d_2 \equiv d \pmod{(p_2 - 1)}$, and

⋮

$d_k \equiv d \pmod{(p_k - 1)}$,

solving said sub-tasks to determine results M_1', M_2', ... M_k', and

combining said results of said sub-tasks to produce said receive message word M', wherein M'=M.

22. (Twice Amended) A cyptographic communications system for establishing communications that are backwards compatible with preexisting public key [infrastructures] transformation schemes, comprising:

a communication medium;

encoding means coupled to said communication medium and adapted for transforming a transmit message word M to a ciphertext word C and for transmitting said ciphertext word C on said medium, wherein M corresponds to a number representative of a message, and

$0 \leq M \leq n-1$, wherein n is a composite number of the form,

$n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$

wherein k is an integer greater than 2 and $p_1, p_2, \ldots, p_k$ are distinct random prime numbers, and wherein said ciphertext word C corresponds to a number representative of an enciphered form of said message and corresponds to

$C \equiv M^e \pmod{n}$,

wherein e is a number relatively prime to (p_1-1), (p_2-1), ..., and (p_k-1); and

decoding means communicatively coupled with said communication medium for receiving said ciphertext word C via said medium, said decoding means being operative to perform a decryption process for transforming said ciphertext word C to a receive message word

M', wherein M' corresponds to a number representative of a deciphered form of C, said decryption process using a decryption exponent d that is defined by

$$d \equiv e^{-1} \bmod ((p_1-1)(p_2-1)\ldots(p_k-1)),$$

said decryption process including the steps of

defining a plurality of k sub-tasks in accordance with

$$M_1' \equiv C_1^{d_1} \pmod{p_1},$$

$$M_2' \equiv C_2^{d_2} \pmod{p_2},$$

$$\vdots$$

$$M_k' \equiv C_k^{d_k} \pmod{p_k},$$

wherein

$$C_1 \equiv C \pmod{p_1},$$

$$C_2 \equiv C \pmod{p_2},$$

$$\vdots$$

$$C_k \equiv C \pmod{p_k},$$

$$d_1 \equiv d \pmod{(p_1 - 1)},$$

$$d_2 \equiv d \pmod{(p_2 - 1)},$$

$$\vdots$$

$$d_k \equiv d \pmod{(p_k - 1)},$$

solving said sub-tasks to determine results M_1', M_2', ... M_k', and

combining said results of said sub-tasks to produce said receive message word M' whereby M'=M.

27. (Twice Amended) A method for establishing cryptographic communications that are backwards compatible with preexisting public key [infrastructures] <u>transformation schemes</u>, comprising the step of:

encoding a plaintext message word M to a ciphertext word C, wherein M corresponds to a number representative of a message, and

$0 \le M \le n-1$,

n being a composite number formed from the product of $p_1 \cdot p_2 \cdot \ldots \cdot p_k$, wherein k is an integer greater than 2 and $p_1, p_2, \ldots, p_k$ are distinct random prime numbers, and wherein the ciphertext word C is a number representative of an encoded form of message word M, wherein said step of encoding includes the steps of

defining a plurality of k sub-tasks in accordance with

$$C_1 \equiv M_1^{e_1} \pmod{p_1},$$

$$C_2 \equiv M_2^{e_2} \pmod{p_2},$$

$$\vdots$$

$$C_k \equiv M_k^{e_k} \pmod{p_k},$$

where

$$M_1 \equiv M \pmod{p_1},$$

$$M_2 \equiv M \pmod{p_2},$$

$$\vdots$$

$$M_k \equiv M \pmod{p_k},$$

$$e_1 \equiv e \pmod{(p_1 - 1)},$$

$$e_2 \equiv e \pmod{(p_2 - 1)}, \text{ and}$$

$$\vdots$$

$$e_k \equiv e \pmod{(p_k - 1)},$$

wherein e is a number relatively prime to (p_1-1), (p_2-1), ..., and (p_k-1),

solving said sub-tasks to determine results $C_1, C_2, \ldots C_k$, and

combining said results of said sub-tasks to produce said ciphertext word C.

32. (Twice Amended) A cyptographic communications system for establishing communications that are backwards compatible with preexisting public key [infrastructures] <u>transformation schemes</u>, comprising:

a communication medium;

encoding means coupled to said communication medium and operative to transform a transmit message word M to a ciphertext word C, and to transmit said ciphertext word C on said medium, wherein M corresponds to a number representative of a message, and

$0 \leq M \leq n-1$,

n being a composite number formed from the product of $p_1 \cdot p_2 \cdot \ldots \cdot p_k$ wherein k is an integer greater than 2 and $p_1, p_2, \ldots, p_k$, are distinct random prime numbers, and wherein the ciphertext word C is a number representative of an encoded form of message word M, said encoding means being operative to transform said transmit message word M to said ciphertext word C by performing an encoding process comprising the steps of

defining a plurality of k sub-tasks in accordance with

$$C_1 \equiv M_1^{e_1} \pmod{p_1},$$

$$C_2 \equiv M_2^{e_2} \pmod{p_2},$$

$$\vdots$$

$$C_k \equiv M_k^{e_k} \pmod{p_k},$$

where

$$M_1 \equiv M \pmod{p_1},$$

$$M_2 \equiv M \pmod{p_2},$$

$$\vdots$$

$$M_k \equiv M \pmod{p_k},$$

$$e_1 \equiv e \pmod{(p_1 - 1)},$$

$$e_2 \equiv e \pmod{(p_2 - 1)}, \text{ and}$$

$$\vdots$$

$$e_k \equiv e \pmod{(p_k - 1)},$$

wherein e is a number relatively prime to (p_1-1), (p_2-1), ..., and (p_k-1),

solving said sub-tasks to determine results $C_1, C_2, \ldots C_k$, and

combining said results of said sub-tasks to produce said ciphertext word C.

37. (Twice Amended) A method for establishing cryptographic communications that are backwards compatible with preexisting public key [infrastructures] transformation schemes, comprising the steps of:

decoding a ciphertext word C to a message word M, wherein M corresponds to a number representative of a message and wherein

$0 \leq M \leq n-1$

wherein n is a composite number formed by the product of $p_1 \cdot p_2 \cdot \ldots \cdot p_k$, k is an integer greater than 2 and $p_1, p_2, \ldots, p_k$ are distinct random prime numbers, C is a number representative of an encoded form of message word M that is encoded by transforming said message word M to said ciphertext word C whereby

$C \equiv M^e \pmod{n}$,

and wherein e is a number relatively prime to (p_1-1), (p_2-1), ..., and (p_k-1);

said decoding step being performed using a decryption exponent d that is defined by

$d \equiv e^{-1} \bmod ((p_1-1)(p_2-1) \ldots (p_k-1))$,

wherein said step of decoding includes the steps of

defining a plurality of k sub-tasks in accordance with

$M_1 \equiv C_1^{d_1} \pmod{p_1}$,

$M_2 \equiv C_2^{d_2} \pmod{p_2}$,

$\vdots$

$M_k \equiv C_k^{d_k} \pmod{p_k}$,

wherein

$C_1 \equiv C \pmod{p_1}$,

$C_2 \equiv C \pmod{p_2}$,

$\vdots$

$C_k \equiv C \pmod{p_k}$,

$d_1 \equiv d \pmod{(p_1 - 1)}$,

$d_2 \equiv d \pmod{(p_2 - 1)}$, and

$\vdots$

$d_k \equiv d \pmod{(p_k - 1)}$,

solving said sub-tasks to determine results $M_1, M_2, \ldots M_k$, and

combining said results of said sub-tasks to produce said message word M.

42. (Twice Amended) A cyptographic communications system for establishing communications that are backwards compatible with preexisting public key [infrastructures] transformation schemes, comprising:

a communication medium;

communicatively coupled with said communication medium for receiving a ciphertext word C via said medium, and being operative to transform said ciphertext word C to a receive message word M', wherein a message M corresponds to a number representative of a message and wherein,

$0 \leq M \leq n-1$

wherein n is a composite number formed by the product of $p_1 \cdot p_2 \cdot \ldots \cdot p_k$, k is an integer greater than 2 and $p_1, p_2, \ldots, p_k$ are distinct random prime numbers, and wherein said ciphertext word C is a number representative of an encoded form of said message word M that is encoded by transforming M to said ciphertext word C whereby,

$C \equiv M^e \pmod{n}$,

and wherein e is a number relatively prime to (p_1-1), (p_2-1), ..., and (p_k-1);

said decoding means being operative to perform a decryption process using a decryption exponent d that is defined by

$d \equiv e^{-1} \bmod ((p_1-1)(p_2-1) \ldots (p_k-1))$,

said decryption process including the steps of

defining a plurality of k sub-tasks in accordance with,

$M_1' \equiv C_1^{d_1} \pmod{p_1}$,

$M_2' \equiv C_2^{d_2} \pmod{p_2}$,

$\vdots$

$M_k' \equiv C_k^{d_k} \pmod{p_k}$,

wherein,

$C_1 \equiv C \pmod{p_1}$,

$C_2 \equiv C \pmod{p_2}$,

$\vdots$

$C_k \equiv C \pmod{p_k}$,

$d_1 \equiv d \pmod{(p_1 - 1)}$,

$d_2 \equiv d \pmod{(p_2 - 1)}$, and

$\vdots$

$d_k \equiv d \pmod{(p_k - 1)}$,

solving said sub-tasks to determine results M_1', M_2', ... M_k', and

combining said results of said sub-tasks to produce said receive message word M', whereby M'=M.

47. (Twice Amended) A method for generating a digital signature <u>that is backwards compatible with preexisting public key transformation schemes,</u> comprising the step of:

signing a plaintext message word M to create a signed ciphertext word C, wherein M corresponds to a number representative of a message, and

$0 \leq M \leq n-1$,

n being a composite number formed from the product of $p_1 \cdot p_2 \cdot \ldots \cdot p_k$, wherein k is an integer greater than 2 and p_1, p_2, ..., p_k are distinct random prime numbers, and wherein the signed ciphertext word C is a number representative of a signed form of message word M, wherein

$C \equiv M^d \pmod{n}$, and

wherein said step of signing includes the steps of

defining a plurality of k sub-tasks in accordance with

$C_1 \equiv M_1^{d_1} \pmod{p_1}$,

$C_2 \equiv M_2^{d_2} \pmod{p_2}$,

$\vdots$

$C_k \equiv M_k^{d_k} \pmod{p_k}$,

where

$M_1 \equiv M \pmod{p_1}$,

$M_2 \equiv M \pmod{p_2}$,

$\vdots$

$M_k \equiv M \pmod{p_k}$,

$d_1 \equiv d \pmod{(p_1 - 1)}$,

$d_2 \equiv d \pmod{(p_2 - 1)}$, and

$\vdots$

$d_k \equiv d \pmod{(p_k - 1)}$,

wherein d is defined by

$d \equiv e^{-1} \bmod ((p_1 - 1) \cdot (p_2 - 1) \cdot \ldots \cdot (p_k - 1))$, and

e is a number relatively prime to (p_1-1), (p_2-1), ..., and (p_k-1),

solving said sub-tasks to determine results C_1, C_2, ... C_k, and

combining said results of said sub-tasks to produce said ciphertext word C.

52. (Twice Amended) A digital signature generation system that is backwards compatible with preexisting public key transformation schemes, comprising:

a communication medium;

digital signature generating means coupled to said communication medium and operative to transform a transmit message word M to a signed ciphertext word C, and to transmit said signed ciphertext word C on said medium, wherein M corresponds to a number representative of a message, and

$0 \leq M \leq n-1$,

n being a composite number formed from the product of $p_1 \cdot p_2 \cdot \ldots \cdot p_k$ wherein k is an integer greater than 2 and p_1, p_2, ..., p_k, are distinct random prime numbers, and wherein the signed ciphertext word C is a number representative of a signed form of said message word M, wherein

$C \equiv M^d \pmod{n}$,

said digital signature generating means being operative to transform said transmit message word M to said signed ciphertext word C by performing a digital signature generating process comprising the steps of,

defining a plurality of k sub-tasks in accordance with,

$$C_1 \equiv M_1^{d_1} \pmod{p_1},$$

$$C_2 \equiv M_2^{d_2} \pmod{p_2},$$

$$\vdots$$

$$C_k \equiv M_k^{d_k} \pmod{p_k},$$

where,

$$M_1 \equiv M \pmod{p_1},$$

$$M_2 \equiv M \pmod{p_2},$$

$$\vdots$$

$$M_k \equiv M \pmod{p_k},$$

$$d_1 \equiv d \pmod{(p_1 - 1)},$$

$$d_2 \equiv d \pmod{(p_2 - 1)}, \text{ and}$$

$$\vdots$$

$$d_k \equiv d \pmod{(p_k - 1)},$$

wherein d is defined by,

$$d \equiv e^{-1} \bmod ((p_1 - 1) \cdot (p_2 - 1) \cdot \ldots \cdot (p_k - 1)), \text{ and}$$

e is a number relatively prime to (p_1-1), (p_2-1), ..., and (p_k-1),

solving said sub-tasks to determine results C_1, C_2, ... C_k, and

combining said results of said sub-tasks to produce said signed ciphertext word C.

57. (Twice Amended) A digital signature process that is backwards compatible with preexisting public key transformation schemes, comprising the steps of:

signing a plaintext message word M to create a signed ciphertext word C, wherein M corresponds to a number representative of a message and wherein

$$0 \leq M \leq n-1$$

wherein n is a composite number formed by the product of $p_1 \cdot p_2 \cdot \ldots \cdot p_k$, k is an integer greater than 2 and p_1, p_2, ..., p_k are distinct random prime numbers, C is a number

representative of a signed form of message word M, and wherein said encoding step comprises transforming said message word M to said ciphertext word C whereby,

$C \equiv M^d \pmod{n}$,

wherein d is defined by

$d \equiv e^{-1} \bmod ((p_1 - 1) \cdot (p_2 - 1) \cdot \ldots \cdot (p_k - 1))$, and

e is a number relatively prime to (p_1-1), (p_2-1), ..., and (p_k-1); and

verifying said ciphertext word C to a receive message word M' by performing the steps of,

defining a plurality of k sub-tasks in accordance with

$$M_1' \equiv C_1^{e_1} \pmod{p_1},$$

$$M_2' \equiv C_2^{e_2} \pmod{p_2},$$

$$\vdots$$

$$M_k' \equiv C_k^{e_k} \pmod{p_k},$$

wherein

$$C_1 \equiv C \pmod{p_1},$$

$$C_2 \equiv C \pmod{p_2},$$

$$\vdots$$

$$C_k \equiv C \pmod{p_k},$$

$$e_1 \equiv e \pmod{(p_1 - 1)},$$

$$e_2 \equiv e \pmod{(p_2 - 1)}, \text{ and}$$

$$\vdots$$

$$e_k \equiv e \pmod{(p_k - 1)},$$

solving said sub-tasks to determine results M_1', M_2', ... M_k', and

combining said results of said sub-tasks to produce said receive message word M', whereby M'=M.

62. (Twice Amended) A digital signature system that is backwards compatible with preexisting public key transformation schemes, comprising:

a communication medium;

digital signature generating means coupled to said communication medium and adapted for transforming a message word M to a signed ciphertext word C and for transmitting said signed ciphertext word C on said medium, wherein M corresponds to a number representative of a message, and

$0 \leq M \leq n-1$, wherein n is a composite number of the form

$n = p_1 \bullet p_2 \bullet \ldots \bullet p_k$,

wherein k is an integer greater than 2 and $p_1, p_2, \ldots, p_k$ are distinct random prime numbers, and wherein said signed ciphertext word C corresponds to a number representative of a signed form of said message word M and corresponds to

$C \equiv M^d \pmod{n}$,

wherein d is defined by

$d \equiv e^{-1} \bmod ((p_1 - 1) \bullet (p_2 - 1) \bullet \ldots \bullet (p_k - 1))$, and

e is a number relatively prime to (p_1-1), (p_2-1), ..., and (p_k-1); and

digital signature verification means communicatively coupled with said communication medium for receiving said signed ciphertext word C via said medium, and being operative to verify said signed ciphertext word C by performing the steps of,

defining a plurality of k sub-tasks in accordance with

$$M_1' \equiv C_1^{e_1} \pmod{p_1},$$

$$M_2' \equiv C_2^{e_2} \pmod{p_2},$$

$$\vdots$$

$$M_k' \equiv C_k^{e_k} \pmod{p_k},$$

wherein

$$C_1 \equiv C \pmod{p_1},$$

$$C_2 \equiv C \pmod{p_2},$$

$$\vdots$$

$$C_k \equiv C \pmod{p_k},$$

$e_1 \equiv e \pmod{(p_1 - 1)}$,

$e_2 \equiv e \pmod{(p_2 - 1)}$,

⋮

$e_k \equiv e \pmod{(p_k - 1)}$,

solving said sub-tasks to determine results M_1', M_2', ... M_k', and

combining said results of said sub-tasks to produce said receive message word M' wherein M'=M.